OIPE JC139 AUG 16 2002 PATENT & TRADEMARK OFFICE

2131

*PATENT*
ATTORNEY DOCKET NO.: 109933.00103

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|---|---|---|
| In re Patent Application of: | ) | |
| | ) | |
| Walter Mason STEWART et al. | ) | |
| | ) | |
| Serial No.: 09/704,790 | ) | Examiner: Not Yet Assigned |
| | ) | |
| Filed: November 3, 2000 | ) | Group Art Unit: 2131 |
| | ) | |
| Title: E-MAIL VIRUS PROTECTION SYSTEM AND METHOD | ) | |

RECEIVED
AUG 2 0 2002
Technology Center 2100

**RENEWED PETITION TO MAKE SPECIAL**

Honorable Commissioner for Patents
Washington, D.C. 20231

Date: August 16, 2002

ATTN: Pinchus M. Laufer
Special Programs Examiner
Technology Center 2100

Sir:

The Applicants hereby renew the petition to make the above-captioned application special under the special examining procedure set forth in 37 C.F.R. §1.102 and MPEP §708.02

The Applicants respectfully submit that the invention disclosed and claimed in the above-captioned patent application is patentable over the references found in the search.

Claims 1-15 are directed to a method for protecting a network from a virus contained in an e-mail message as executable code. As recited in claim 1, step (b), the executable code is converted from an executable format to a non-executable format. The e-mail message containing executable virus code is converted to a different computer format that, while it can retain the semantic content of the original e-mail, cannot be executed by the target computer. As recited in step (c), the non-executable format is forwarded to the recipient of the e-mail message.

DUPLICATE OF #5

Claims 16-30 are directed to a system corresponding to the method of claims 1-15. As recited in claim 16, the computer on the network converts the executable code from an executable format to a non-executable format and forwards the non-executable format to a workstation computer used by a recipient of the e-mail message.

Claims 31-41 recite a sacrificial server usable in the method of claims 1-16 or the system of claims 16-30. The server comprises processing means for converting the e-mail attachment from an executable format to a non-executable format and for returning the e-mail attachment to the network.

The present claimed invention offers advantages over known techniques for e-mail virus protection. By converting the attachment from an executable format to a non-executable format, the present claimed invention protects against unknown viruses, which virus scanners may miss. Also, time may be of the essence in communicating the information in the attachment to the recipient, so that it is desirable to forward the attachment to the recipient in the non-executable format rather than simply to delete or quarantine the attachment. For example, a Microsoft Word document, which may contain a macro virus, can be converted to an Adobe Acrobat PDF file, which will be safe. Other advantages are described in the originally filed specification on pp. 3 and 4.

The cited references do not anticipate the present claimed invention. Further, no combination of the cited references would have rendered the present claimed invention obvious. The four most closely relevant references will be described; then, the differences between them and the present claimed invention will be identified.

*Thacker* '696 teaches a virus trap connected between a computer and a network for preventing a virus from entering the computer from the network. Also provided is a fully

isolated test computer, called a "safe house." A virus in a transferred file, such as an e-mail attachment, passes through the virus trap on its way to the user's computer. The virus may run and destroy sacrificial data in the virus trap. However, the virus trap includes failsafe technology (not disclosed in detail) which enables it to recover. Also, programs that the user downloads intentionally can be detected and sent to the safe house.

*Chen et al* '208 teaches a software agent for detecting and removing computer viruses located in attachments to e-mail messages. If an e-mail message has an attachment, the attachment is detached and sent to an anti-virus application for scanning. If the attachment is determined to have a virus, it can be deleted, and an alert may be generated.

*Ji et al* '943 teaches a system for the detection and elimination of viruses in e-mail and FTP transfers. If a virus is detected, the server can, according to a configuration file, transfer the file, delete the file, or store the file and notify the user of the file name and directory path from which the file can be manually requested.

"Declude Virus" teaches an anti-virus package which interacts directly with a mail server. The description is of particular interest because the stated purpose of the package is to reduce the number of servers involved in processing mail, thus teaching away from the present invention.

As can be seen from the above, none of the cited references teaches or even remotely suggests the conversion of the executable code from an executable format to a non-executable format. In *Thacker*, the "safe house," which appears to be the closest thing to the sacrificial server or the computer on the network as recited in the present claims, performs no such function. Also, *Thacker* does not protect from a virus spoofing or escaping from either the "*virus trap*" or "*safe house*". The other references do not overcome the deficiencies of *Thacker,* since

they discuss simply passing, deleting, or storing a file rather than converting it as done in the present claimed invention.

The other cited references are deemed to be of general interest and are considered to be even less relevant to the present claimed invention.

As none of the cited references teaches or suggests the conversion of the executable code from an executable format to a non-executable format, it is clear that none of the cited references anticipates any of the present claims.

Further, none of the cited references would have rendered the present claimed invention obvious. A person having ordinary skill in the art who had reviewed the references would not have been given motivation, or have been taught the desirability, of modifying any of the references to incorporate conversion of the executable code into a non-executable format and forwarding the non-executable format, rather than simply passing, deleting, or storing the file as received. Instead, the only teaching or suggestion to do so comes from the present invention.

Finally, no combination of the cited references would have rendered the present claimed invention obvious. Even if for some reason a person having ordinary skill in the art had been motivated to combine any or all of the references, such a combination would still not have included any conversion of executable code to non-executable format and forwarding of the non-executable format.

For the reasons set forth above, the Applicants respectfully submit that the above-captioned application should be made special. Notice that the above-captioned application has been made special is earnestly solicited.

Please charge any deficiency in fees, or credit any overpayment thereof, to BLANK ROME COMISKY & McCAULEY LLP, Deposit Account No. 23-2185 (109933.00103).

Respectfully submitted,

Walter Mason STEWART et al.

By:_____
David J. Edmondson
Reg. No. 35,126

BLANK ROME COMISKY & MCCAULEY LLP
900 17th Street, N.W., Suite 1000
Washington, D.C. 20006
Phone: (202) 530-7400
Fax: (202) 463-6915